Symantec™ Event Relay for IBM Tivoli Risk Manager Integration Guide

Symantec™ Event Relay for IBM Tivoli Risk Manager Integration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0

Copyright Notice

Copyright © 2002 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. SESA, Symantec Enterprise Security Architecture, and Symantec Security Response are trademarks of Symantec Corporation.

IBM, Tivoli, and Tivoli Enterprise Console are trademarks of the IBM Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to you. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

A. use that number of copies of the Software as have been licensed to you by Symantec under a License Module for your internal business purposes. If no License Module accompanies, precedes, or follows this license, you may make one copy of the Software you are authorized to use on a single machine.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;

C. use each licensed copy of the Software on a single central processing unit; and

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; nor

F. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms

are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Technical support

Chapter 1 Introducing Symantec Event Relay

Who should read this guide 10
What you should know 10
About the Symantec Event Relay for IBM Tivoli Risk Manager 10
How the Symantec Event Relay processes events 11

Chapter 2 Installing the Symantec Event Relay

Installation overview 14
SESA component installation 14
    Installing the Symantec Event Relay softwarei 15
    Configuring the TEC servlet 15
    Filtering events sent to Tivoli 17
    Changing the default event mapping 18
Tivoli Event Server installation 18
    Configuring the T/EC server rule base for SESA events 19
    Configuring the T/EC console 19
Troubleshooting the Symantec Event Relay after installation 22
    Verifying SESA operation 22
    Examining SESA log files 22
    Modifying TEC servlet properties 23
Uninstalling the Symantec Event Relay for IBM Tivoli Risk Manager 25
    Uninstalling the Symantec Event Relay from the SESA Manager 25
    Uninstalling Symantec Event Relay files from Tivoli 26

Appendix A Event Mapper file format specification

Event blocks 28
Event mapping criteria 29
Default event block 30
Event Mapper file modifications 31
Tag reference 31

Appendix B Default event mappings

SESA_Unscannable_Incident 36
SESA_Content_Incident 37
RMV_VirusFound 38
SESA_Scan_Start 39
SESA_Scan_End 40
SESA_Scan_Pause 41
SESA_Scan_Resume 42
SESA_Scan_Cancel 43
SESA_App_Update_Event 44
RMV_VirusDBUpdated 45
RMV_VirusDBUpdated (failure) 46
SESA_Defs_Update_Event 47
SESA_Config_Update_Event 48
SESA_Network_Event 49
SESA_Advisory_Malware_Event 50
SESA_Activity_Malware_Event 51
SESA_Event_Generic 52

Index

Chapter 1

Introducing Symantec Event Relay

This chapter includes the following topics:

- Who should read this guide
- What you should know
- About the Symantec Event Relay for IBM Tivoli Risk Manager
- How the Symantec Event Relay processes events

Who should read this guide

This guide is intended for Tivoli administrators and SESA administrators who will install, configure, and use the Symantec Event Relay for IBM Tivoli Risk Manager.

What you should know

You should have prior knowledge of Tivoli Management Framework, Tivoli Enterprise Console (T/EC), and Tivoli Risk Manager. You should also be familiar with basic SESA operation and event logging.

For more information, see the following documentation:

- *Symantec Enterprise Security Architecture Installation Guide*
- *Symantec Enterprise Security Architecture Administrator's Guide*

About the Symantec Event Relay for IBM Tivoli Risk Manager

SESA is an event management system that collects data from events generated by security products. SESA categorizes events into classes such as antivirus, content filtering, network security, and systems management. The range of events varies depending on the security products.

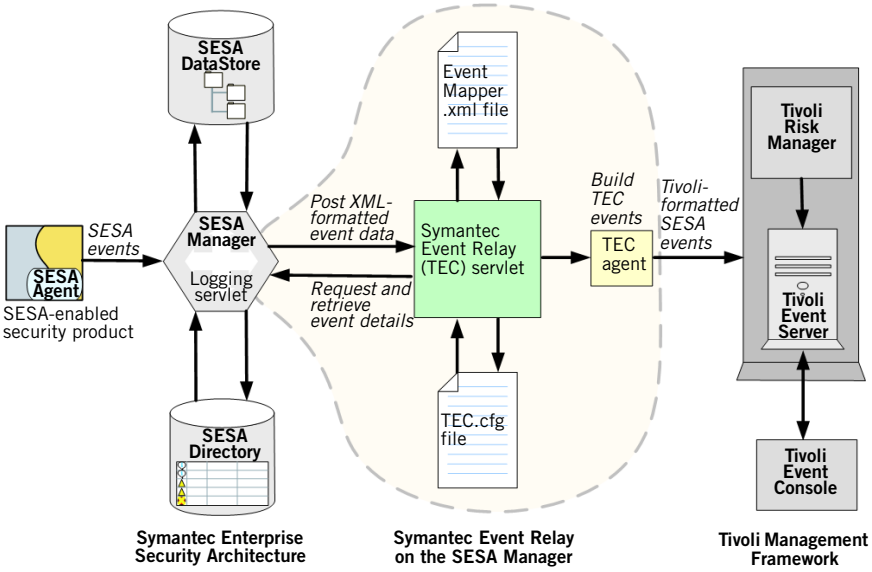
The events conform to an extensible family of event classes and types, which are defined by sets of XML schema. Once collected, event information is stored in the SESA DataStore for access by SESA management functions through the SESA Console.

The Symantec Event Relay for IBM Tivoli Risk Manager is an event adapter that lets the Tivoli Enterprise Console and Tivoli Risk Manager manage events that originate from SESA sources. The Symantec Event Relay captures events that are sent to SESA, maps these events to the proper format for the Tivoli environment, and forwards the events to the Tivoli Risk Manager for access through Tivoli Event Consoles.

How the Symantec Event Relay processes events

Figure 1-1 shows the main components of the Symantec Event Relay and indicates the flow of event data through those components.

Figure 1-1 Symantec Event Relay for IBM Tivoli Risk Manager



The data flow begins with event data from a SESA-enabled security product. The SESA Agent that is installed on the security product computer sends event data to the SESA logging servlet on the SESA Manager computer. Once the event data is validated and saved to the SESA DataStore, the SESA logging servlet sends the data to the Symantec Event Relay (TEC) servlet. The TEC servlet is an executable Java module that runs on the SESA Manager computer. At installation, the TEC servlet is configured to locate the Tivoli Event Server by IP address and port number.

The TEC servlet does the following:

- Receives the posted XML event data from the SESA logging servlet.
- Optionally, filters SESA event data.
- Maps the XML data to the Tivoli event class structure. This mapping is necessary for SESA-posted data to be converted to T/EC formatted data. The EventMapper.xml file contains the instructions for mapping SESA events to Tivoli events.

For information on how this file is organized and how to make changes, see "Event Mapper file format specification" on page 27.

- Requests detailed information about an event from the SESA database, if necessary.
- Formats the event data.
- Forwards the event data to Tivoli Risk Manager, which contains the event class structures and event definitions that Tivoli needs to identify incoming event data from the Symantec Event Relay.

Tivoli SecureWay Risk Manager runs on the Tivoli Event Console server that is specified in the TEC.cfg file.

Chapter 2

Installing the Symantec Event Relay

This chapter includes the following topics:

- Installation overview
- SESA component installation
- Tivoli Event Server installation
- Troubleshooting the Symantec Event Relay after installation
- Uninstalling the Symantec Event Relay for IBM Tivoli Risk Manager

Installation overview

You must perform the following two separate sets of procedures to install the Symantec Event Relay:

- SESA component installation: Install and configure the Symantec Event Relay components and TEC servlet on the SESA Manager computer.
- Tivoli Event Server installation: Install and configure the Symantec Event Relay event class definition files on the Tivoli Event Server. Configure the Tivoli Event Console.

You can perform either sequence first.

The Sun Java Development Kit (JDK), which is already installed as part of SESA installation, runs the Symantec Event Relay installation on the SESA Manager computer.

For the Tivoli Event Server, event class definition files, or .baroc files, define the types and structures of the events that the Tivoli Event Server can receive. The CreateSesaRB.sh script adds an event class definition file for SESA events (SESA.baroc), and recompiles and reloads the rule base. This lets the Tivoli Event Server recognize and display events that originate from SESA-managed applications.

SESA component installation

Before installing the Symantec Event Relay, ensure that the SESA Manager, SESA Directory, SESA DataStore, and the Tivoli Event Server are installed and running. This installation assumes that all SESA components are operating properly.

Installing and configuring the Symantec Event Relay on the SESA Manager involves performing the following procedures:

- Installing the Symantec Event Relay softwarei
- Configuring the TEC servlet

If necessary, you can perform the following optional procedures:

- Filtering events sent to Tivoli
- Changing the default event mapping

Installing the Symantec Event Relay software

The Symantec Event Relay is installed on the computer that hosts the SESA Manager.

To install the Symantec Event Relay software

1. On the computer on which the SESA Manager is installed, from Windows Explorer, navigate to the folder that contains the Symantec Event Relay Setup.jar file (the SESA Integration Wizard).

   Setup.jar resides in the \install\sesa folder.

2. Double-click **Setup.jar** to begin the SESA Integration Wizard.

3. The SESA Integration Wizard prompts you for specific information.

SESA Domain Administrator Name	The SESA Directory Domain Administrator account name. This account is created either during SESA installation or after installation from within SESA.
SESA Domain Administrator Password	The administrator password.
IP address or hostname of the SESA Directory	Use one of the following: ■ The IP address of the SESA Directory. Use the IP address if SESA is installed with the default, anonymous self-signed SSL certificate. ■ The hostname of the SESA Directory. Use the hostname if SESA is upgraded to use an authenticated, self-signed SSL certificate or Certificate Authority-signed SSL certificate.
SSL port	The SSL port for the SESA Directory (by default, 636).

4. When the SESA Integration Wizard completes, click **Finish**.

Configuring the TEC servlet

TEC servlet operation is governed by the TEC servlet configuration file (TEC.cfg), which resides on the SESA Manager computer.

Performing the following tasks allows you to set the configuration in the TEC.cfg file and confirm operation:

- Configuring the TEC.cfg file
- Verifying TEC servlet operation

Configuring the TEC.cfg file

The TEC.cfg configuration file is a text file that must be edited in a text editor (for example, Notepad).

To configure the TEC.cfg file

1. On the computer on which the SESA Manager is installed, from a command prompt, navigate to the TECServlet folder.
   The following is the default location:
   \Program Files\IBM HTTP Server\Tomcat\Webapps\TECServlet
2. In the TECServlet folder, open the TEC.cfg file in a text editor.
3. Modify the TEC.cfg file so that it contains the required information.

ServerLocation	The T/EC server name. For example: ServerLocation=tec.mycompany.com You can type the server name or IP address.
ServerPort	The server port. The default port for Windows NT/2000 T/EC servers is 5529. The default for UNIX T/EC servers is 0. For example: ServerPort=5529 If your T/EC server is listening on another port, type the appropriate port.
BufEvtPath	The location for the temporary buffer cache. In the following example, cache is the name of the cache file: BufEvtPath=c:/temp/cache Create the directory for the cache file if it doesn't already exist. Use forward slashes to specify the path in the TEC.cfg file. The BufEvtPath keyword sets the filename used for event buffering in case the Symantec Event Relay is unable to connect to the Tivoli Enterprise Console. Set the path to a location that has enough disk space available for the buffered events. Note that only non-filtered events are buffered.

Lines in the TEC.cfg file that begin with the number sign (#) are comments.

4 Save the modified TEC.cfg file.
The new settings are loaded automatically.

Note: Additional configuration settings, which may be required in your environment, can be specified in the TEC.cfg file. For a complete listing and description of the available configuration keywords, see *Tivoli Enterprise Console Adapters Guide*.

Verifying TEC servlet operation

After modifications are made to the TEC.cfg file, verify that the TEC servlet is operating.

To verify TEC servlet operation

1 Open Internet Explorer and type the following case-sensitive URL:
https://localhost/TECServlet/servlet/TECServlet
Use localhost if you are on the same computer as the SESA Manager, or replace localhost with the IP address or host name of the SESA Manager.

2 When you are prompted, type the SESA Domain Administrator logon and password information.
Internet Explorer displays the TECServlet information page.

Filtering events sent to Tivoli

Event filters from SESA to Tivoli are based on attribute=value pairs and regular expression matching. To filter events that SESA sends to Tivoli, use the Filter, FilterCache, and FilterMode keywords in the TEC.cfg file.

For example, to prevent SESA from sending generic events to Tivoli, use the following keywords:

- FilterMode=OUT
- Filter:Class=SESA_Event_Generic

For more information, see the "Configuration File, Keywords" section of the *Tivoli Enterprise Console Adapters Guide*.

Changing the default event mapping

Event mappings between SESA events and Tivoli events are specified in the Event Mapper XML file. Generally, you do not have to change the mappings.

By default, the EventMapper.xml file is located in the TECServlet installation folder:

\Program Files\IBM HTTP Server\Tomcat\Webapps\TECServlet

For information on how this file is organized and how to make changes, see "Event Mapper file format specification" on page 27.

To review the mappings that are included with the default installation of the Symantec Event Relay, see "Default event mappings" on page 35.

Tivoli Event Server installation

For the Tivoli Event Server to receive SESA event information, you must run the script that recompiles the Tivoli event class definition files on the Tivoli Event Server to include information on SESA events.

Before installing the Symantec Event Relay, ensure that the following Tivoli components are installed and operating properly:

- Tivoli Management Framework 3.7.1
- Tivoli Enterprise Console 3.7.1 (Server, UI Server, and Console)
- Tivoli SecureWay Risk Manager 3.8

Performing the following procedures allows you to install the SESA event class definition file (SESA.baroc) on the Tivoli Event Server:

- Configuring the T/EC server rule base for SESA events
- Configuring the T/EC console

Configuring the T/EC server rule base for SESA events

SESA-generated events are described for the T/EC rule base in the SESA.baroc file. The CreateSesaRB.sh script automatically adds and compiles the event classes from the SESA.baroc file.

To configure the T/EC server rule base for SESA events

1. On the T/EC server, open a command prompt or shell with the Tivoli paths and Tivoli environment set.
2. Insert the Symantec Event Relay CD into the CD-ROM drive.
3. Change to the install\riskmgr folder.
4. Type the following command:

   sh CreateSesaRB.sh

   Upon successful completion of the CreateSesaRB.sh script, the Tivoli rule base accepts SESA events.

Configuring the T/EC console

The Symantec Event Relay includes a configuration file that is imported into the T/EC console to define a Tivoli event group for SESA events.

Performing the following procedures allows you to configure and use the T/EC console:

- Creating a Tivoli event group for SESA events
- Assigning and using the SESA event group
- Viewing SESA events

Creating a Tivoli event group for SESA events

The sesa_event_group.cfg file contains information to create a Tivoli event group for SESA events.

To create a Tivoli event group for SESA events

1. Open and log on to the T/EC console.
2. In the Tivoli Enterprise Console, on the Windows menu, click **Configuration.**
3. On the File menu, click **Import**.
4. Click **Browse**, then navigate to the sesa_event_group.cfg file.
   The sesa_event_group.cfg file is located in the install\riskmgr folder.
5. Select **sesa_event_group.cfg**, then click **Select**.
6. In the Event Groups panel, click **SESA Relay**, then click **OK**.
7. When prompted that the T/EC console must be shut down and restarted for the changes to take place, click **OK**.
8. Restart the T/EC console.

Assigning and using the SESA event group

After the Tivoli event group for SESA events is created, it must be assigned to a console before it can be used.

To assign and use the SESA event group

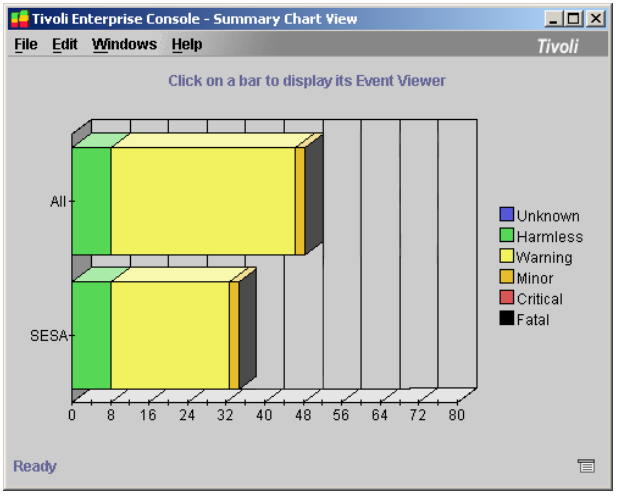
1. Open and log on to the T/EC console.
2. In the Tivoli Enterprise Console, on the Windows menu, click **Configuration.**
3. In the left pane, expand **Consoles**, then select the desired console.
4. Open the selected console, right-click **Event Groups**, then click **Assign Event Groups**.
5. Click **Assign Groups**, then click **SESA Relay** from the Available Event Groups list.
6. In the Event Group Roles list on the right, assign the SESA Relay privileges, then click **OK.**
   The operators for that console can now see SESA in their summary chart view and event viewer.
7. Click **OK** to close the Console Properties dialog box.

Viewing SESA events

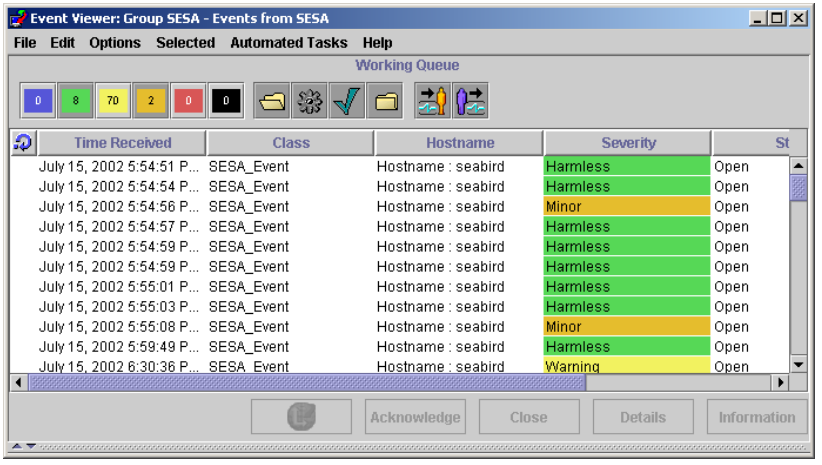
After the event group is created and assigned, operators for the console can view SESA events.

To view SESA events

1 In the T/EC console, on the Windows menu, click **Summary Chart View**.



2 In the Summary Chart View, click a bar to display its event viewer.


Event Viewer: Group SESA - Events from SESA
File Edit Options Selected Automated Tasks Help
Working Queue
0 8 70 2 0 0
Time Received Class Hostname Severity St
July 15, 2002 5:54:51 P... SESA_Event Hostname : seabird Harmless Open
July 15, 2002 5:54:54 P... SESA_Event Hostname : seabird Harmless Open
July 15, 2002 5:54:56 P... SESA_Event Hostname : seabird Minor Open
July 15, 2002 5:54:57 P... SESA_Event Hostname : seabird Harmless Open
July 15, 2002 5:54:59 P... SESA_Event Hostname : seabird Harmless Open
July 15, 2002 5:54:59 P... SESA_Event Hostname : seabird Harmless Open
July 15, 2002 5:55:01 P... SESA_Event Hostname : seabird Harmless Open
July 15, 2002 5:55:03 P... SESA_Event Hostname : seabird Harmless Open
July 15, 2002 5:55:08 P... SESA_Event Hostname : seabird Minor Open
July 15, 2002 5:59:49 P... SESA_Event Hostname : seabird Harmless Open
July 15, 2002 6:30:36 P... SESA_Event Hostname : seabird Warning Open
Acknowledge
Close
Details
Information

Troubleshooting the Symantec Event Relay after installation

If the Symantec Event Relay installation fails, performing the following procedures allows you to confirm operation:

- Verifying SESA operation
- Examining SESA log files
- Modifying TEC servlet properties

Verifying SESA operation

You can verify SESA operation by confirming that the proper services and the Web server are running.

To verify SESA operation

1. On the computer running the SESA Manager, open the Services Control Panel and verify that the following services are running:
   - IBM HTTP Server
   - SESA AgentStart Service
   - Apache Tomcat
2. In Internet Explorer, type the following URL and log on using SESA Domain Administrator credentials:

   https://localhost/sesa/servlet/EventLogger

   Make sure that the SESA Event Logger summary is displayed in Internet Explorer. If not, SESA may not be properly configured.

Examining SESA log files

If all of the necessary services are started (including SES AgentStart) and you can see the SESA Event Logger, but the Symantec Event Relay still does not work, check the SESA log files for the Event Logger servlet.

To examine SESA log files

1. Open the SESA log files from the following locations:
   ...\SESA\<computer name>\Events\logs
   ...\SESA\<computer name>\TECServlet\logs
2. Check for the return code value coming back from the Tivoli Risk Manager server.
   The return code should be 0, with the following message:
   TEC_TargetTivoli : Event sent to target system, return code = 0. A return code of 0 indicates success.
   If the return code is non-zero, there may be a problem communicating with the Tivoli Risk Manager server.

   Note: Success messages are reported only if the Debug setting is ON. If the the Debug setting is OFF, only non-zero failure messages are reported. To set Debug ON or OFF, see "Modifying TEC servlet properties" on page 23.
3. Verify that the SESA.baroc file has been compiled and loaded by the CreateSesaRB.sh script, and that the server is running.

Modifying TEC servlet properties

To resolve some issues, you may need to modify the TEC servlet properties.

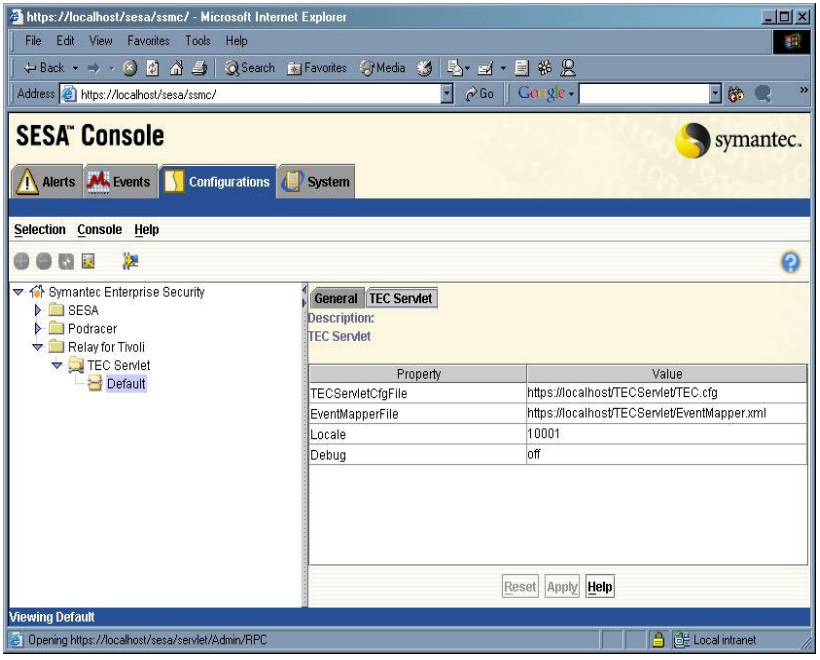
Modification of the SESA Directory TEC servlet configuration properties is optional. The defaults listed in the following table should work without modification:

Property	Description
URL for the TEC.cfg file	http://localhost/TECServlet/TEC.cfg
URL for EventMapper.xml	http://localhost/TECServlet/EventMapper.xml
Debug setting	OFF (default): Normal operation. Only error conditions are logged. ON: Extensive debug logging is performed. By default, the log is written to the following location: \SESA\<SESA Manager>\TECServlet\logs\<guid>\<guid>.log

Property	Description
Locale setting	■ 10001 (English — default) ■ 10002 (French) ■ 10003 (Italian) ■ 10004 (German) ■ 10005 (Spanish) ■ 10006 (Portuguese) ■ 10007 (Dutch) ■ 10008 (Japanese) ■ 10009 (Simplified Chinese) ■ 10010 (Traditional Chinese) ■ 10011 (Korean)

To modify TEC servlet properties

1. In the SESA Console, on the Configurations tab, in the left pane, navigate to **Symantec Enterprise Security > Relay for Tivoli> TEC Servlet > Default.**
2. In the right pane, on the TEC Servlet tab, change the settings as necessary.



Uninstalling the Symantec Event Relay for IBM Tivoli Risk Manager

Removing the Symantec Event Relay involves performing the following two tasks:

- Uninstalling the Symantec Event Relay from the SESA Manager
- Uninstalling Symantec Event Relay files from Tivoli

Because the files and configurations that are installed on the Tivoli Risk Manager and T/EC server are inactive unless they receive SESA events, it is not critical to uninstall these components.

Uninstalling the Symantec Event Relay from the SESA Manager

The SESA Integration Wizard that installs the Symantec Event Relay is also used to uninstall it.

To uninstall the Symantec Event Relay from the SESA Manager

1. On the computer running the SESA Manager, insert the Symantec Event Relay for IBM Tivoli Risk Manager CD into the CD-ROM drive.
2. At a command prompt, change to the install\sesa folder.
3. Type the following command to launch the SESA Integration Wizard:
   java –jar setup.jar –uninstall
4. Follow the on-screen instructions.
5. On the panel that requests SESA Domain Administrator information, provide the same information that was used when SESA was originally installed.

SESA Domain Administrator Name	The SESA Directory Domain Administrator account name. This account is created either during SESA installation or after installation from within SESA.
SESA Domain Administrator Password	The administrator password.

IP address or hostname of the SESA Directory	Use one of the following: ■ The IP address of the SESA Directory. Use the IP address if SESA is installed with the default, anonymous self-signed SSL certificate. ■ The hostname of the SESA Directory. Use the hostname if SESA is upgraded to use an authenticated, self-signed SSL certificate or Certificate Authority-signed SSL certificate.
SSL port	The SSL port for the SESA Directory (by default, 636).

The SESA Integration Wizard performs the uninstallation and removal of the Symantec Event Relay for IBM Tivoli Risk Manager. The TECServlet folder is removed if it is empty.

Uninstalling Symantec Event Relay files from Tivoli

You can uninstall the components on the Tivoli servers if necessary.

To uninstall Symantec Event Relay from Risk Manager and the T/EC server

1. From the T/EC console configuration, delete the SESA event group.
2. Remove the SESA-specific event classes (SESA.baroc) from the current rule base, or modify the active rule base to not include SESA.baroc.
   See the Tivoli user documentation for more information.

Appendix A

Event Mapper file format specification

This section contains the following topics:

- Event blocks
- Event mapping criteria
- Default event block
- Event Mapper file modifications
- Tag reference

The Symantec Event Relay uses an Event Mapper file that consists of a list of event blocks. Each event block defines a set of criteria for mapping a particular SESA event to an event for the destination environment.

Note: The EventMapper.xml file must be saved in UTF-8 format.

Event blocks

The Event Mapper file should contain at least one event block. Each event block has the following general structure:

```
<EVENT>
    <TARGETCLASS NAME="" />
    <CRITERIA>
        <CLASS NAME=""/>
        <PROPERTY NAME="" VALUE=""/>
            .
            .
            .
    </CRITERIA>
    <LOCALE NAME="">
        <SLOT TARGET_NAME="">
            <APPEND STRING=""/>
            <APPEND SOURCE_NAME=""/>
            <APPEND SOURCE_NAME=""  LOCALE=""/>
                .
                .
                .
        </SLOT>
            .
            .
            .
    </LOCALE>
</EVENT>
```

Event mapping criteria

Each event block can, optionally, specify mapping criteria that identify the conditions under which the Symantec Event Relay should use the event block for mapping. These mapping criteria are stored in a criteria block within the event block. The class name and property values for the source SESA event must match the entries specified in this criteria block in order for the event to be mapped to the target event specified in the event block. If the source event meets the criteria defined for multiple event blocks, the first block found will be used to map the event.

The following example is an event block that contains mapping criteria:

```
<EVENT>
    <TARGETCLASS NAME="RMV_VirusFound" />
    <CRITERIA>
        <CLASS NAME="symc_virus_violation"/>
        <PROPERTY NAME="machine" VALUE="stellars"/>
        <PROPERTY NAME="event_id" VALUE="301"/>
    </CRITERIA>
    <LOCALE NAME="101">
        <SLOT TARGET_NAME="msg">
            <APPEND STRING="Virus found : "/>
            <APPEND SOURCE_NAME="virus_name"/>
        </SLOT>
        .
        .
        .
    </LOCALE>
</EVENT>
```

According to the criteria block, if the source event has a class name of symc_virus_violation, a machine property with the value “stellars,” and an event_id property with the value “301,” the event will be mapped to the specified target class of RMV_VirusFound.

The locale is read from the property file for the TEC servlet. The locale block contains a sequence of slot blocks that are used to build the strings to be associated with the target events.

The following example is a formatted string that is sent to the msg slot for this event block:

Virus found: MK4 killer in file myFile.doc on Nov 30, 2001, 3:30:00 PST.
Action: Repaired.
Event Type: Application start.
Event GUID: cf6891b054f7f53e0ea55ea84fe0002

Default event block

An event block that does not contain mapping criteria is used as a default event mapping; that is, the mapping for this event block is used when the source event does not meet the criteria specified for the other event blocks in the Event Mapper file.

The Event Mapper file should provide a default mapping. The default event mapping must be at the end of the file.

The following is an example of a default event block:

```
<EVENT>
    <TARGETCLASS NAME="SESA_Event" />
    <LOCALE NAME="101">
        <SLOT TARGET_NAME="msg">
            <APPEND STRING="An event occurred on "/>
            <APPEND SOURCE_NAME="event_dt"/>
            <APPEND STRING=".  Severity : "/>
            <APPEND SOURCE_NAME="severity_id"  LOCALE="101"/>
            <APPEND STRING=".  Hostname : "/>
            <APPEND SOURCE_NAME="machine" />
            <APPEND STRING=".  Host IP Addr : "/>
            <APPEND SOURCE_NAME="origin"/>
        </SLOT>
        .
        .
        .
    </LOCALE>
</EVENT>
```

Event Mapper file modifications

Because the Event Mapper file is text-based, you can add new event blocks or delete or modify existing event blocks, if desired.The Event Mapper file can be modified using a text editor, such as Notepad, that supports writing files in UTF-8 format.

If the format of the Event Mapper file is invalid, the TEC servlet ignores the contents of the file and will not map incoming SESA events. When the file is parsed, the TEC servlet indicates the event block number and information about the problematic tag. Errors are noted in the TECServlet log files on the SESA server.

See "Examining SESA log files" on page 22.

Tag reference

Note the following format restrictions that govern the EventMapper.xml file:

- The header line must exist only once.
- The opening <EventList> tag must be on a line by itself, immediately following the header line.
- The opening <Event> tag must be on a line by itself.
- All closing tags should exist on lines by themselves.
- The following blocks must exist on one line with the shortened closing tag syntax, as shown in the following example:
  <TARGETCLASS NAME=" " />
  <CLASS NAME=" " />
  <PROPERTY NAME=" " VALUE=" " />
  <APPEND STRING=" " />
  <APPEND SOURCE_NAME=" " />
  In the <CRITERIA> block, a <CLASS> block must be placed before any <PROPERTY> blocks.

Tag	Description
<EVENT></EVENT>	Defines an event block. The Event Mapper file should contain at least one event block, and should contain a default event mapping.

Tag	Description
`<TARGETCLASS NAME=" "/>`	Designates the target (destination) class name to which events in the source class will be mapped. There can be only one of these blocks per event block.
`<CRITERIA></CRITERIA>`	Defines the criteria block for the current event. The criteria block is used to determine whether this event block will be used for mapping a given source event. This block is optional, but if present, there can be no more than one criteria block in a given event block. If there are no criteria blocks for this event, this event is the default map event, to be used when none of the other event blocks has criteria that match the source event.
`<CLASS NAME=" "/>`	Defines an event class name to be matched against the source event. There must be one and only one of these blocks per criteria block.
`<PROPERTY NAME=" " VALUE=" "/>`	Defines a property name and value pair to be matched against the source event. This block is optional, and there can be up to 10 property blocks per criteria block.
`<LOCALE NAME=" "></LOCALE>`	Defines the mapping for a particular locale. For example, the name value might be 10001 (English). At least one block must exist. There can be up to 10 of these blocks.
`<SLOT TARGET_NAME=" ">`	Defines the T/EC slot to which the formatted information will be sent. The formatted information is a text string that is built by following the instructions in the append blocks. Each slot must have at least one append block. There can be up to 50 slot blocks per locale block. There can be up to 100 append blocks per slot block.
`<APPEND STRING=" "/>`	Specifies a string to be concatenated to the current message string.
`<APPEND SOURCE_NAME=" "/>`	Specifies a property name for the source event. The value of this property is concatenated to the current message string.

Tag	Description
`<APPEND SOURCE_NAME="" LOCALE="" />`	Specifies a property name for the source event. The value of this property is an identifier that is used for a database query according to the given locale. The value retrieved from the database will be concatenated to the current message string.

Appendix B

Default event mappings

This section describes the event mappings that are defined by the default EventMapper.xml file. For details on the syntax and semantics of this file, see "Event Mapper file format specification" on page 27.

Note: For the Tivoli Event Console to receive these events correctly, the EventMapper.xml target event schema must match that of the .baroc files on the T/EC server.

When specifying <APPEND SOURCE_NAME=" " /> blocks, several fields receive special translation when being processed by the Symantec Event Relay.

Field	Description
event_dt_fmt	Is translated into a human-readable representation of the Event Date based on the Locale setting for the Symantec Event Relay
event_dt_raw	Is translated into a hex representation of the Event Date in seconds since EPOCH
sensor_machine	Receives the machine name of the computer running the Symantec Event Relay (the SESA Manager)
sensor_machine_ip	Receives the IP address of the computer running the Symantec Event Relay (the SESA Manager)
severity	Maps the SESA severity number into an appropriate Tivoli severity number

Some Tivoli event slots are set by the Risk Manager rules when the event is received. The names and descriptions of these fields can be found in the *Tivoli Risk Manager Developer's Guide*. These fields should not be specified in the EventMapper.xml or SESA.baroc file because they will be overwritten by Tivoli.

SESA_Unscannable_Incident

Event criteria

SESA Class Name = "symc_data_incident"

SESA Property Name : event_id = "112056"

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> found in : '<**data_name**>' on <**event_dt_fmt**>. Unscannable reason : '<**data_rule_reason**>'.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**> : <**event_id (translated)**>
rm_Object	Data Name : '<**data_name**>' Part name : '<**data_part_name**>'
sesa_RuleDescription	<**data_rule_descr**>
sesa_RuleReason	<**data_rule_reason**>
sesa_ProductName	<**product_id (translated)**> : <**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Content_Incident

Event criteria

SESA Class Name = "symc_data_incident"

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> was found in '<**data_name**>' on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
rm_Object	Data Name : '<**data_name**>' Part name : '<**data_part_name**>'
sesa_RuleDescription	Rule Description : <**data_rule_descr**>
sesa_RuleReason	Reason : <**data_rule_reason**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

RMV_VirusFound

Event criteria

SESA Class Name = "symc_data_virus_incident"

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> : '<**data_rule_reason**>' was found in '<**data_name**>' on <**event_dt_fmt**>. The current status of this data is : <**data_status_id (translated)**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**> : <**event_id (translated)**>
rm_Virus	<**data_rule_reason**>
rm_VirusFileInfected	Data Name : '<**data_name**>' Part name : '<**data_part_name**>'
rm_VirusAction_Desc	Current Data Status : <**data_status_id (translated)**>

SESA_Scan_Start

Event criteria

SESA Class Name = "symc_data_scan"

SESA Property Name : event_id = "112051"

Default destination event fields (slots)

Target name	Default setting
msg	Scan : '<**data_scan_name**>' started on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ScanName	<**data_scan_name**>
sesa_ScanType	<**data_scan_type_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Scan_End

Event criteria

SESA Class Name = "symc_data_scan"

SESA Property Name : event_id = "112052"

Default destination event fields (slots)

Target name	Default setting
msg	Scan : '<**data_scan_name**>' ended on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ScanName	<**data_scan_name**>
sesa_ScanType	<**data_scan_type_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Scan_Pause

Event criteria

SESA Class Name = "symc_data_scan"

SESA Property Name : event_id = "112053"

Default destination event fields (slots)

Target name	Default setting
msg	Scan : '<**data_scan_name**>' was paused on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ScanName	<**data_scan_name**>
sesa_ScanType	<**data_scan_type_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Scan_Resume

Event criteria

SESA Class Name = "symc_data_scan"

SESA Property Name : event_id = "112054"

Default destination event fields (slots)

Target name	Default setting
msg	Scan : '<**data_scan_name**>' resumed on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ScanName	<**data_scan_name**>
sesa_ScanType	<**data_scan_type_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Scan_Cancel

Event criteria

SESA Class Name = "symc_data_scan"

SESA Property Name : event_id = "112055"

Default destination event fields (slots)

Target name	Default setting
msg	Scan : '<**data_scan_name**>' was canceled on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ScanName	<**data_scan_name**>
sesa_ScanType	<**data_scan_type_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_App_Update_Event

Event criteria

SESA Class Name = "symc_app_update"

Default destination event fields (slots)

Target name	Default setting
msg	Application : '<**product_id (translated)**>' was updated on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_PrevVer	<**prev_version**>
sesa_CurrVer	<**curr_version**>
sesa_EventGuid	<**event_guid**>

RMV_VirusDBUpdated

Event criteria

SESA Class Name = "symc_defupdate"

SESA Property Name : event_id = "92004"

Default destination event fields (slots)

Target name	Default setting
msg	Virus definitions updated on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>

RMV_VirusDBUpdated (failure)

Event criteria

SESA Class Name = "symc_defupdate"

SESA Property Name : event_id = "92054"

Default destination event fields (slots)

Target name	Default setting
msg	Virus definition update failed on <**event_dt_fmt**>.
rm_Result	Failure
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**> : <**event_id (translated)**>

SESA_Defs_Update_Event

Event criteria

SESA Class Name = "symc_defupdate"

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> occurred on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_PrevVer	<**prev_version**>
sesa_CurrVer	<**curr_version**>
sesa_EventGuid	<**event_guid**>

SESA_Config_Update_Event

Event criteria

SESA Class Name = "symc_config_update"

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> occurred on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**> : <**event_id (translated)**>
rm_Object	Config Name : <**config_name**>
sesa_CurrVer	<**config_revision**>
sesa_ProductName	<**product_id (translated)**> : <**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Network_Event

Event criteria

SESA Class Name = "symc_network"

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> occurred on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**> : <**event_id (translated)**>
rm_Object	Config Name : <**config_name**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Advisory_Malware_Event

Event criteria

SESA Class Name = "symc_advisory_malware"

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> occurred on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Activity_Malware_Event

Event criteria

SESA Class Name = "symc_activity_malware"

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> occurred on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

SESA_Event_Generic

Event criteria

<NONE>

Default destination event fields (slots)

Target name	Default setting
msg	<**event_id (translated)**> was found on <**event_dt_fmt**>.
rm_SensorType	SESA Relay for T/EC
rm_SensorHostname	<**sensor_machine**>
rm_SensorIPAddr	<**sensor_machine_ip**>
rm_SourceHostname	<**machine**>
rm_SourceIPAddr	<**machine_ip**>
rm_DestinationHostname	<**machine**>
rm_DestinationIPAddr	<**machine_ip**>
adapter_host	<**sensor_machine**>
rm_Timestamp	<**event_dt_raw**>
severity	<**severity**>
rm_Description	<**event_id (translated)**>
rm_Signature	<**eventclass_id (translated)**>:<**event_id (translated)**>
sesa_ProductName	<**product_id (translated)**>:<**swfeature_id (translated)**>
sesa_EventGuid	<**event_guid**>

Index

A

anonymous, self-signed SSL certificates 15
assigning SESA event groups 20
authenticated, self-signed SSL certificates 15

C

Certificate Authority-signed SSL certificates 15
changing the default event mapping 18
components of the Symantec Event Relay 11
configuration file 19
configuring
    T/EC console 19
    T/EC server rule base for SESA events 19
    TEC servlet 15
    TEC.cfg file 16
creating Tivoli event groups for SESA events 19

D

Debug setting 23
default event block 30
default event mappings, about 35
Domain Administrator name 15
Domain Administrator password 15

E

event blocks 28
event filtering 17
event management 10
Event Mapper file format
    default event block 30
    event blocks 28
    event mapping criteria 29
    modifications 31
    specification 27
    tag reference 31
Event Mapper XML file 18
event mappings
    changing the default 18
    criteria 29
    default 35
    RMV_VirusDBUpdated 45
    RMV_VirusDBUpdated (failure) 46
    RMV_VirusFound 38
    SESA_Activity_Malware_Event 51
    SESA_Advisory_Malware_Event 50
    SESA_App_Update_Event 44
    SESA_Config_Update_Event 48
    SESA_Content_Incident 37
    SESA_Defs_Update_Events 47
    SESA_Event_Generic 52
    SESA_Network_Event 49
    SESA_Scan_Cancel 43
    SESA_Scan_End 40
    SESA_Scan_Pause 41
    SESA_Scan_Resume 42
    SESA_Scan_Start 39
    SESA_Unscannable_Incident 36
event processing for the Symantec Event Relay 11
examining SESA log files 22

F

file format modifications, Event Mapper 31
file format specification
    default event block 30
    event blocks 28
    Event Mapper 27
    event mapping criteria 29
filtering events 17

I

installation
- overview 14
- SESA components 14
- Symantec Event Relay software 14, 15
- Tivoli Event Server 14, 18
- troubleshooting 22

L

log files, examining 22

M

modifying
- Event Mapper file 31
- TEC servlet properties 23

O

overview of installation 14

P

password, Domain Administrator account 15
properties, modifying for TEC servlet 23

R

return code 23
rule base, configuring for T/EC server 19

S

server port 16
SESA
- component installation 14
- Domain Administrator name 15
- Domain Administrator password 15
- event groups, assigning and using 20
- events
  - configuring the T/EC server rule base 19
  - viewing 21
- log files, examining 22
- operation, verifying 22

SESA Manager, uninstalling the Symantec Event Manager from 25
SESA.baroc file 19
sesa_event_group.cfg file 19
specifications
- default event block 30
- event blocks 28
- Event Mapper file format 27
- event mapping criteria 29

SSL certificates
- anonymous, self-signed 15
- authenticated, self-signed 15
- Certified Authority-signed 15

Symantec Event Relay for IBM Tivoli Risk Manager
- about 10
- components 11
- event processing 11
- installation 14, 15
- uninstalling files from Tivoli 26
- uninstalling from the SESA Manager 25

T

T/EC
- about 10
- console, configuring 19
- server rule base, configuring for SESA events 19

tag reference for Event Mapper file 31
TEC servlet
- about 11
- configuring 15
- modifying properties 23
- verifying operation 17

TEC.cfg 16
TECServlet
- folder 16
- information page 17

Tivoli
- event groups, creating for SESA events 19
- uninstalling the Symantec Event Manager files from 26

Tivoli Enterprise Console 10
Tivoli Event Server installation 14, 18
Tivoli Management Framework 10
troubleshooting installation 22

U

uninstalling
    Symantec Event Relay files from Tivoli 26
    Symantec Event Relay from the SESA Manager 25
UNIX 16
using SESA event groups 20

V

verifying
    SESA operation 22
    TEC servlet operation 17
viewing SESA events 21

W

Windows NT/2000 16